UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CA 92278-8100

CCO 5230.3B
6
JAN 26 2015

COMBAT CENTER ORDER 5230.3B

From: Commanding General
To: Distribution List

Subj: ESTABLISHING AND MAINTAINING SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) COMPUTER NETWORK CONNECTIVITY ABOARD THE COMBAT CENTER

Ref: (a) DoDM 5200.01 Volumes 1-4, "DoD Information Security Program", February 24, 2012
(b) DoD Instruction 8500.1, "Cybersecurity"' March 14, 2014
(c) SECNAV M-5510.36
(d) MCO 5530.14A
(e) MARADMIN 288/13
(f) MARADMIN 590/05
(g) CCO 5532.1B
(h) 29 Palms SIPRNET Authority to Operate (ATO)/Authority to Connect (ATC)

Encl: (1) CC 2620/1 SIPRNET Change Request
(2) Flowchart
(3) CC 2620/2 Sonic Change Request

1. Situation. The Combat Center's Secret Internet Protocol Router Network (SIPRNET) system infrastructure is persistently subjected to and threatened by external and internal information technology threats. The references provide guidance and policies on the security measures needed to operate, maintain, and protect SIPRNET equipment and data against illicit or accidental modification, destruction, disclosure, or denial of service as well as on the handling, storing, labeling, and classification of that data to include physical and electronic types and their respective containers.

2. Cancellation. CCO 5230.3A.

3. Mission. Promulgate procedures and responsibility for commanding officers, assistant chiefs of staff (AC/S), special staff officers, and appointed personnel to establish, maintain, operate, and govern user accessibility to the Combat Center SIPRNET.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All established SIPRNET seats, system administrators, and personnel, granted access to the Marine Air Ground Task Force Training Command (MAGTFTC), Marine Corps Air Ground Combat Center (MCAGCC) SIPRNET domain, will strictly adhere to the procedures set forth in this Order. Failure to do so may create a breach of national security and result in punitive measures.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

(2) Concept of Operations. The Combat Center SIPRNET domain is defined as the classified computer network, administered by the MAGTFTC, MCAGCC AC/S G-6, Communication and Information Systems for communication up to "SECRET" classified information via the Marine Corps Enterprise Network (MCEN). All connections must be obtained and maintained per this Order.

b. Subordinate Element Missions

(1) Chief of Staff. Approve or disapprove restricted area requests.

(2) AC/S G-6

(a) Provide contract oversight, customer technical representation, and onsite operational liaison with the SIPRNET Project Manager (PM) aboard the Combat Center.

(b) Identify SIPRNET domain resource requirements for annual budgets and ensure resources are in compliance with higher headquarters directives and policies.

(3) SIPRNET PM

(a) Provide Requesting Agent with a sample SIPRNET standard operating procedures (SOP) specific to the system.

(b) Provide Requesting Agent initial Change Request feasibility determination.

(c) Ensure the Connection Approval Process is successful.

1. Assign Internet Protocol (IP) addresses to the unit.

2. Ensure a physical network connection to the unit exists.

(d) Maintain an appropriate security posture for the mission at hand.

(e) Maintain all required MCEN SIPRNET domain and seat accreditation documentation for active seats.

(f) Maintain a SIPRNET Authority to Operate and Connect (ATO/ATC).

(4) Information Systems Security Manager (ISSM)

(a) Provide staff cognizance of the MCEN SIPRNET domain, seat Certification and Accreditation (C&A) for all organizations utilizing the Combat Center SIPRNET domain.

(b) Review all SIPRNET seat requests for compliance with component directives and policies.

(c) Review and approve all required MCEN SIPRNET domain and seat accreditation documentation for active seats.

(d) Coordinate issuance of the ATO/ATC with the PM when all requirements are met.

(e) Ensure SIPRNET assets are scanned for vulnerabilities to ensure that all Security Technical Implementation Guides and software patches are applied and updated.

(f) Ensure Host Based Security System is loaded and configured on each server and workstation to detect malicious computer-related activities.

(g) Sign SIPRNET System Authorization Access Requests (SAARs).

(5) Requesting Unit (Commanding Officer (CO) or designated representative)

(a) Complete the SIPRNET Change Request Survey, Enclosure (1), and attach it in an email to the G-6 Service Desk (SMBPLMSHelpDesk@usmc.mil) along with the following supporting documentation:

1. CO Request. If this is a new classified area without an existing SIPRNET drop/jack, then a letter or e-mail from the CO to the AC/S G-6 must be attached.

2. SIPRNET SOP. Develop an SOP that identifies physical security, information security, personnel security, and communications security procedures, signed by the Commanding Officer or Director. A sample SOP may be provided by the AC/S G-6 SIPRNET PM. The SOP must include the following procedures:

a. Tasks assigned to billets to safeguard classified information, information processing system, and the KG-175 tactical local area network encryption (TACLANE).

b. Access control based on "need-to-know".

c. Periodic inspections.

d. Utilization of removable secondary storage media and devices.

e. Control of security container combinations.

f. Emergency removal and destruction of classified material.

(b) Network Diagram. The network diagram must identify all hardware information (make, model, hostname, and IP address) of all devices that are requesting connection to the network.

(c) Sonic Change Request. If a new SIPRNET workstation is required then Enclosure (3), Sonic Change Request, must be completed and attached.

(d) TACLANE. Units are required to provide their own TACLANE device to connect to the SIPRNET.

(6) Unit Security Manager

(a) Validate classified information storage areas by ensuring the SIPRNET seat requests meet the designated space as a vault, Secure Room (SR), Controlled Access Area (CAA), or Restricted Access Area (RAA) requirements per references (a) through (d).

(b) Create and maintain classified area certification letters, and as required, revoke certifications for security violation(s).

(c) As required, grant or deny waivers as warranted, for deficiencies cited in the physical security survey conducted by the Provost Marshal Office (PMO).

(d) Provide initial and annual access briefs, North Atlantic Treaty Organization (NATO) secret briefings, and maintain command access rosters to record briefings.

(e) Sign SIPRNET SAARs.

(f) Provide assistance in completing the unit SIPRNET SOP.

(7) PMO

(a) Conduct physical security surveys as required for Open Secret Storage areas per references (a), (b), and (c).

(b) Forward the completed physical security survey with cited deficiencies to requestor and a copy to the unit security manager and ISSM.

c. Coordinating Instructions

(1) Refer to the flowchart in Enclosure (2) for the required steps to establish SIPRNET connectivity.

(2) Requirements for Maintaining SIPRNET Services

(a) To retain SIPRNET access, all SIPRNET users must annually complete the on-line Cyber Awareness Training on MarineNet or Total Workforce Management System, depending on their status, per reference (e).

(b) Unit security managers are responsible for the initial and annual access briefings, NATO Secret briefings, signing the SAAR, and maintaining command access rosters to record the briefings.

(c) All SIPRNET assets must be connected to the SIPRNET the third Wednesday of each month for eight hours to receive software updates. This is a requirement. Failure to do so will result in the SIPRNET assets being placed in quarantine.

5. Administration and Logistics

a. Distribution directives issued by the Commanding General are distributed via email upon request and can be viewed at: http://www.29palms.marines.mil/Staff/G1Manpower/AdjutantOffice/Orders.aspx.

b. Forms. Enclosure (1) is the CC 2620/1 SIPRNET Change Request 2620/1 and enclosure (3) is the CC 2620/2 Sonic Change Request. They can be obtained from the Naval Forms Online web site at https://navalforms.documentservices.dla.mil/web/public/home. Use the forms tab to access the search page; the number or title can be entered in the keyword search. All former editions are obsolete and will not be accepted.

6. Command and Signal

a. Command. This order is applicable to all Combat Center personnel and organizations requesting and being granted access to the Combat Center SIPRNET domain.

b. Signal. This Order is effective the date signed.

J. B. HANLON
Chief of Staff

Distribution: A

SIPRNET CHANGE REQUEST

1. Requesting Agent Information:

a. Unit

b. Point of Contact:

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

c. Information Systems Coordinator (ISC) or Terminal Area Security Officer (TASO)

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

d. Security Manager

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

2. Has the security manager certified the area to process classified information?	□ Yes (attach copy of certifying letter)	□ No
3. Are there pre-existing SIPRNET services in the space?	□ Yes	□ No
4. Are any devices a Program of Record (POR)?	□ Yes	□ No
5. Has a SONIC asset been ordered or identified?	□ Yes	□ No
6. Is there an existing jack for the new requirement?	□ Yes	□ No

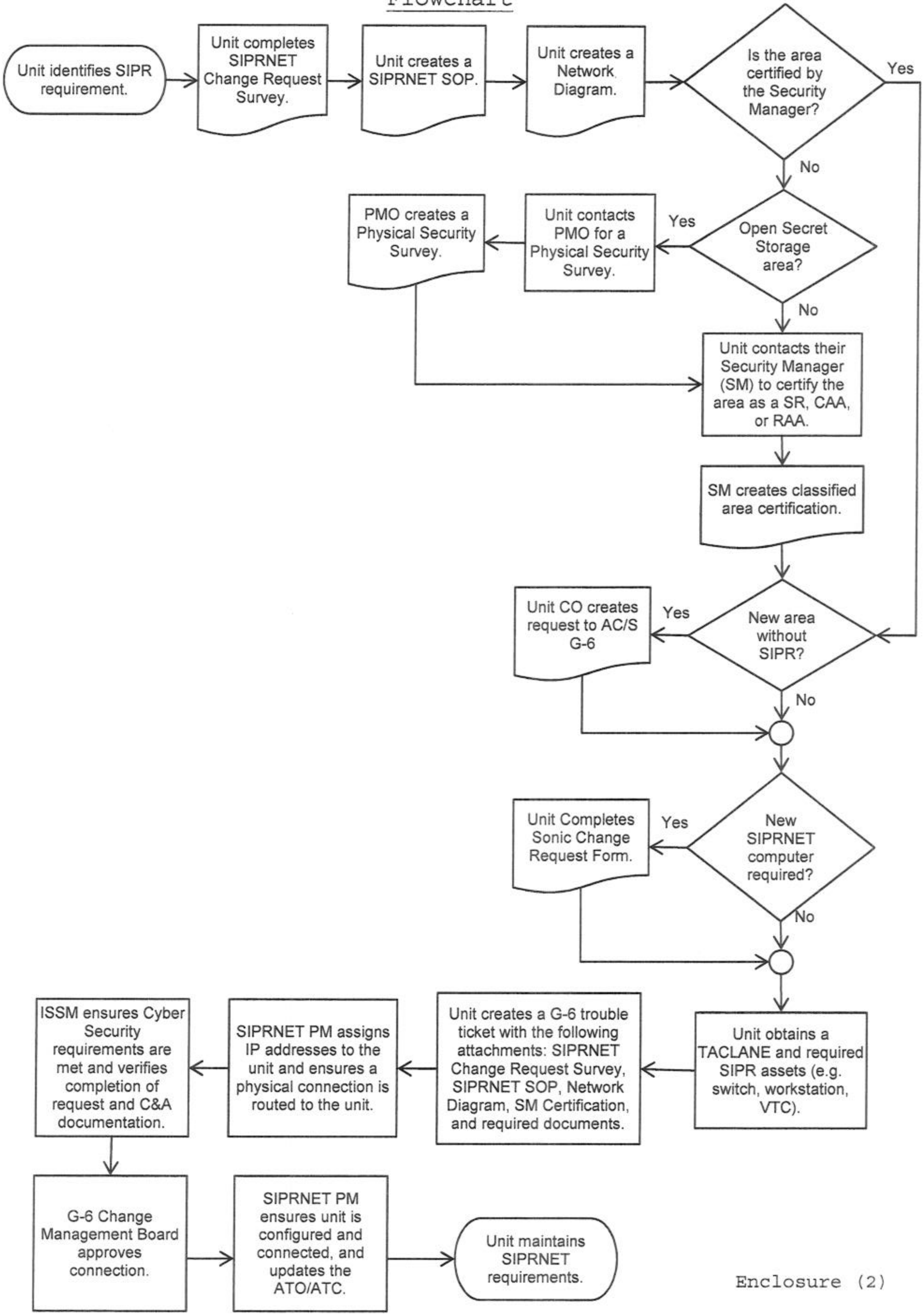
7. Identify the purpose of the seats being requested

8. As the Requesting Agent, I will ensure service request requirements are properly coordinated with the MAGTFTC, MCAGCC G-6, and the authorized system remains in compliance with CCO 5230.3 (series) and references, and the SIPRNET Program Manager.

Requesting Agent Signature

Date Signed

Flowchart


Unit identifies SIPR requirement.
Unit completes SIPRNET Change Request Survey.
Unit creates a SIPRNET SOP.
Unit creates a Network Diagram.
Is the area certified by the Security Manager?
Yes
No
Open Secret Storage area?
Yes
Unit contacts PMO for a Physical Security Survey.
PMO creates a Physical Security Survey.
No
Unit contacts their Security Manager (SM) to certify the area as a SR, CAA, or RAA.
SM creates classified area certification.
New area without SIPR?
Yes
Unit CO creates request to AC/S G-6
No
New SIPRNET computer required?
Yes
Unit Completes Sonic Change Request Form.
No
Unit obtains a TACLANE and required SIPR assets (e.g. switch, workstation, VTC).
Unit creates a G-6 trouble ticket with the following attachments: SIPRNET Change Request Survey, SIPRNET SOP, Network Diagram, SM Certification, and required documents.
SIPRNET PM assigns IP addresses to the unit and ensures a physical connection is routed to the unit.
ISSM ensures Cyber Security requirements are met and verifies completion of request and C&A documentation.
G-6 Change Management Board approves connection.
SIPRNET PM ensures unit is configured and connected, and updates the ATO/ATC.
Unit maintains SIPRNET requirements.

SONIC CHANGE REQUEST

1. Title of Request

2. Submission Date

3. Request Type □ New □ Refresh

4. NDAA Required □ Yes □ No

5. J & A Required □ Yes □ No

6. Requester's Name

7. Requester's E-Mail Address

8. Requester's Phone Number

9. Command/Unit POC

10. Command/Unit POC E-Mail Address

11. Detailed Description of Requirement Request

12. Impact if Requirement is not Approved:

13. Date Equipment is Required

14. Comments/Rationale for Required Date:

15. Equipment [illegible] Quantity

16. List and attach any supporting documents.

CC 2620/2 (01-15) PREVIOUS EDITIONS OBSOLETE

Adobe LiveCycle Designer ES2